



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/735,992

12/15/2003

Amer Hassan

M1103.70182US00

2966

45840

7590

02/22/2008

WOLF GREENFIELD (Microsoft Corporation)  
C/O WOLF, GREENFIELD & SACKS, P.C.  
600 ATLANTIC AVENUE  
BOSTON, MA 02210-2206

EXAMINER

GELAGAY, SHEWAYE

ART UNIT

PAPER NUMBER

2137

MAIL DATE

DELIVERY MODE

02/22/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/735,992	<b>Applicant(s)</b> HASSAN ET AL.	
	<b>Examiner</b> SHEWAYE GELAGAY	<b>Art Unit</b> 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 21 November 2007.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-19, 25-33 and 44-51 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-19, 25-33 and 44-51 is/are rejected.
- 7) ☒ Claim(s) 2, 18 and 26 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1. This office action is in response to Applicant's amendment filed on November 21, 2007. Claims 2, 25, 26, 29 and 47 have been amended. Claims 1-19, 25-33 and 44-51 are pending.

#### ***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 47-51 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Regarding claim 47, the phrase "that may be used" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by "may be"), thereby rendering the scope of the claim(s) unascertainable. See MPEP § 2173.05(d).

#### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 3-4, 10-15, 19, 25, 27-28 and 44-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hassan et al. (hereinafter Hassan) US Patent Number 6,031,913 in view of Rastegar et al. (hereinafter Rastegar) US Publication Number 2004/0091054.

As per claims 1, 10 and 25:

Hassan teaches a method of wirelessly generating a cryptographic key that may be used to encrypt wireless communications between a first host and a second host, the method comprising the steps of:

selecting an initial modulation scheme for wireless transmission between the first host and the second host; (col. 3, line 31-col. 4, line 2)

transmitting via the initial modulation scheme first data to be used in generating the cryptographic key; (col. 3, line 31-col. 4, line 2)

receiving via the second modulation scheme second data to be used in generating the cryptographic key; (col. 3, line 31-col. 4, line 2)

generating the cryptographic key using the first and the second data. (col. 3, line 31-col. 4, line 2)

Hassan does not explicitly transmitting an indication of a second modulation scheme. Rastegar in analogous art, however, discloses transmitting an indication of a second modulation scheme. (page 1, paragraphs 11, 16-18) Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by Hassan with Rastegar in order to establish key sequences that depend on physical process with reduced susceptibility to eavesdropping. (Abstract; Hassan)

As per claims 11 and 46:

The combination of Hassan and Rastegar teaches all the subject matter as discussed above. In addition, Hassan further discloses wherein the step of transmitting data comprises the step of: transmitting via the third modulation scheme third data to be used in generating the cryptographic key and an indication of a fourth modulation scheme; (col. 4, line 3-col. 5, line 3)

As per claim 3, 14, 19 and 27:

The combination of Hassan and Rastegar teaches all the subject matter as discussed above. In addition, Hassan further discloses a method comprising the steps of:

determining a desired modulation scheme for wireless communications between the first host and the second host; (Abstract; col. 3, line 1-col. 5, line 3)

encrypting wireless data to be transmitted using the cryptographic key; (Abstract; col. 3, line 1-col. 5, line 3) and

transmitting the encrypted wireless data via the desired modulation scheme.  
(Abstract; col. 3, line 1-col. 5, line 3)

As per claim 4, 13 and 28:

The combination of Hassan and Rastegar teaches all the subject matter as discussed above. In addition, Hassan further discloses determining a size of the cryptographic key; (col. 8, lines 54-62) monitoring an amount of data exchanged; (col. 8, lines 54-62; col. 11, line 31-col. 12, line 24) and selecting a final modulation scheme for a final data exchange between the first host and the second host such that an amount

of data conveyed by the final modulation scheme added to the amount of data exchanged equals the size of the cryptographic key. (col. 8, lines 54-62; col. 11, line 31-col. 12, line 24)

As per claim 12 and 15:

The combination of Hassan and Rastegar teaches all the subject matter as discussed above. In addition, Hassan further discloses comprising the steps of: receiving modulated information; and demodulating the modulated information via the next modulation scheme to extract the data. (col. 8, lines 54-62; col. 11, line 31-col. 12, line 24)

As per claim 44:

The combination of Hassan and Rastegar teaches all the subject matter as discussed above. In addition, Hassan further discloses comprising: randomly selecting the second modulation scheme. (col. 8, lines 5-21)

As per claims 45:

The combination of Hassan and Rastegar teaches all the subject matter as discussed above. In addition, Hassan further discloses wherein: the first data comprises a first set of bits comprising at least one bit; the second data comprises a second set of bits comprising at least one bit; and generating the cryptographic key using the first and the second data comprises combining the first set of bits and the second set of bits. (col. 3, line 31-col. 4, line 2)

6. Claims 5-7, 16-17 and 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hassan et al. (hereinafter Hassan) US Patent Number 6,031,913 in view of Rastegar et al. (hereinafter Rastegar) US Publication Number 2004/0091054 and further in view of Diffie et al. (hereinafter Diffie) US Patent Number 5,371,794.

As per claim 5, 16 and 29:

The combination of Hassan and Rastegar teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein the step of selecting an initial modulation scheme comprises the step of sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme. Diffie in analogous art, however, discloses wherein the step of selecting an initial modulation scheme comprises the step of sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme. (col. 10, lines 25-41) Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by Hassan and Rastegar with Diffie in order to provide a system that prevents key change messages from being played back, without resort to sequence numbers. (col. 10, lines 65-67; Diffie)

As per claim 6, 17 and 30:

The combination of Hassan, Rastegar and Diffie teaches all the subject matter as discussed above. In addition, Diffie further discloses wherein the step of sharing a short key established by a public key method comprises the step of sharing a short key established by a Diffie-Hellman key exchange method. (col. 10, lines 25-41)

As per claim 7 and 31:

The combination of Hassan, Rastegar and Diffie teaches all the subject matter as discussed above. In addition, Diffie further discloses a key exchange method of sending and receiving messages in a wireless network using certificate digitally signed by a certificate authority. (col. 10, lines 65-67; Diffie)

7. Claims 8-9 and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hassan et al. (hereinafter Hassan) US Patent Number 6,031,913 in view of Rastegar et al. (hereinafter Rastegar) US Publication Number 2004/0091054 and further in view of Kim et al. (hereinafter Kim) US Publication Number 2003/0081690.

As per claim 8 and 32:

The combination of Hassan and Rastegar teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein the step of selecting an initial modulation scheme comprises the step of selecting an initial constellation. Kim in analogous art, however, discloses wherein the step of selecting an initial modulation scheme comprises the step of selecting an initial constellation. (page 3, paragraphs 44-45) Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by Hassan and Rastegar with Kim in order to map a predetermined modulation scheme to an initial transmission and retransmissions. (Page 3, paragraph 45; Kim)

As per claims 9 and 33:

The combination of Hassan and Rastegar teaches all the subject matter as discussed above. Both references do not explicitly disclose wherein the step of selecting an initial modulation scheme comprises the step of selecting an initial bit



assignment for a constellation. Kim in analogous art, however, discloses wherein the step of selecting an initial modulation scheme comprises the step of selecting an initial bit assignment for a constellation. (page 3, paragraphs 44-45) Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by Hassan and Rastegar with Kim in order to map a predetermined modulation scheme to an initial transmission and retransmissions. (Page 3, paragraph 45; Kim)

### ***Allowable Subject Matter***

8. Claims 47-51 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.
9. Claims 2, 18 and 26 are objected to as being dependent upon a rejected base claims, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

### ***Response to Arguments***

10. Applicant's arguments see Remarks, filed November 21, 2007, with respect to claims 2, 18, 26 and 47 have been fully considered and are persuasive. The rejection of claims 2, 18, 18, 26 and 47-51 has been withdrawn.

### ***Conclusion***

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay  
/S. G./  
Examiner, Art Unit 2137

/Emmanuel L. Moise/  
Supervisory Patent Examiner, Art Unit 2137